CLAIMS:

2 independent claims, 1, 7, and 5 dependent claims, 2, 3, 4, 5, 6.

What is claimed is:

1. A process for the secure transmission of information over a medium (36), using identical one time pads (28) which are present at a plurality of stations (22) which communicate over said medium, the process comprising the steps of:

(a) providing each said station with a pseudorandom number sequence generator (26) which can generate a pseudorandom number sequence (28) having properties and number sequence programmed and controlled by a replaceable element set (24) which defines and specifies said pseudorandom number sequence;

(b) providing each said station with said replaceable element set, with all of said plurality of stations having identical said replaceable element sets;

(c) allowing each of said plurality of stations to use said pseudorandom number sequence generator and said replaceable element set to generate said pseudorandom number sequence for use as said one time pad;

(d) providing each said station with a mixing technique (30) wherein a plaintext message (34) can be encrypted by means of using said mixing technique to combine said plaintext message and said one time pad;

thereby producing a ciphertext message (32) which can be securely transmitted over said medium;

(e) providing each said station with an inverse mixing technique (42) wherein said ciphertext message can be decrypted by means of using said inverse mixing technique to combine said ciphertext message and said one time pad;

thereby reproducing the original said plaintext message at any of said plurality of stations.

2. The process of claim 1, if said replaceable element set is shorter than said pseudorandom number sequence and said one time pad, it is useful to securely transmit said replaceable element set over said medium as an encrypted message,

allowing for the creation of multiple alternate pseudorandom number sequences at any of said stations,

and allowing the use of said multiple alternate pseudorandom number sequences as multiple alternate one time pads at any of said stations,

whereby any of said stations can receive said multiple alternate one time pads as encrypted traffic over said medium,

providing said stations with fresh and unique versions of said one time pads without the use of a separate and secure distribution path for said one time pads.

3. The process of claim 1, since said replaceable element set is used with said pseudorandom number sequence generator to produce said pseudorandom number sequence and said one time pad,

and since alternate formats of said replaceable element sets and said pseudorandom number sequence generators can be used,

allowing the creation of multiple logical groups of said stations in which all said stations in each of said logical groups share at least one common said alternate format,

whereby said logical groups can, by design, be allowed access or be denied access to other logical groups.

4. The process of claim 1, since said replaceable element set is used with said pseudorandom number sequence generator to produce said pseudorandom number sequence,

and since the use of differing formats of replaceable element sets and differing formats of pseudorandom number sequence generators will produce pseudorandom number sequences having differing properties of randomness and unpredictability and sequence length,

the creation of pseudorandom number sequences having differing properties of randomness and unpredictability and sequence length is possible by varying the formats of said replaceable element sets and said pseudorandom number sequence generators.

5. The process of claim 1, since said replaceable element set is used with said pseudorandom number sequence generator to produce said pseudorandom number sequence,

and since the pseudorandom number sequence which is produced is a function of the starting point of the pseudorandom number sequence,

it is possible to create multiple pseudorandom number sequences from a single replaceable element set by using different starting points for each of said multiple pseudorandom number sequences.

6. The process of claim 1, wherein said process of secure communication contains the step of sending along with the ciphertext message, a set of state information regarding the internal condition of said pseudorandom number sequence generator at the beginning of the encryption process of said ciphertext message.

7. A process for the secure transmission of information over a medium, wherein a plurality of stations intercommunicate over said medium, where the cipher system used in said secure transmission process uses expendable data resources (52) which are diminished with use, and where one or more of said plurality of stations is an originator station (44) and has available to said originator station a source of truly random data (46), and where said originator station or said originator stations can employ a creation technique (50) to operate on truly random data (48) from said source of truly random data or said sources of truly random data and use said truly random data to create new versions of said expendable data resources, and where;

(d) said originator station or said originator stations can transmit to other said stations, as encrypted traffic over said medium, said new versions of said expendable data resources;

whereby said process of secure transmission of information over said medium can continue and be regenerated depending on only the continued presence of said source of truly random data at said originator station or said originator stations;
and whereby any need for said expendable data resources coming from sources external to said plurality of stations is eliminated.